Lesson 03: Be Internet Strong

Secure Your Secrets

Getting real about privacy and security

Lesson overview

Activity 1: **How to build a great password**
Activity 2: **Keep it to yourself**
Activity 3: **Interland: Tower of Treasure**

Themes

Online privacy and security issues don't always have clear right and wrong solutions. Protecting your personal and private information – all the stuff that makes you *you* – means asking the right questions and finding your own educated answers.

Goals for students

- ✓ **Learn** why privacy matters, and how it relates to online security.
- ✓ **Practice** how to create strong passwords.
- ✓ **Review** the tools and settings that protect against hackers and other threats.

Standards addressed

ISTE Standards for Educators: 1a, 2c, 3b, 3c, 3d, 4b, 6a, 6d, 7a
ISTE Standards for Students 2016: 1c, 1d, 2b, 2d, 3d, 6a
AASL Learning Standards: I.b.2, I.c.1, I.c.3, II.c.1, III.a.2, III.b.1, III.c.1, III.d.1, III.d.2, IV.b.3, V.d.3, VI.a.1, VI.d.1

Secure Your Secrets
Vocabulary

Privacy: Protecting people's data and personal information (also called sensitive information)

Security: Protecting people's devices and the software on them

Two-step verification (also called two-factor verification and two-step authentication): A security process where logging in to a service requires two separate steps or two "factors," such as a password and a one-time code. For example, you may have to enter your password and then enter a code that was texted to your phone or a code from an app.

Password or passcode: A secret combination used to access something. It may take different forms; for example, you may have a four-digit number-only code that you use for your phone lock and a much more complex password for your email account. In general, you should make your passwords as long and complex as you can while still being able to remember them.

Encryption: The process of converting information or data into a code that makes it unreadable and inaccessible

Complexity: The goal when creating a secure password. For example, a password is complex when it has a mix of numbers, special characters (like "$" or "&"), and both lowercase and uppercase letters.

Hacker: A person who uses computers to gain unauthorized access to other people's or organizations' devices and data

Secure Your Secrets: Activity 1

How to build a great password

Students learn how to create a strong password – and make sure it stays private after they create it.

Goals for students

- ✓ **Recognize** the importance of never sharing passwords, except with parents or guardians.
- ✓ **Understand** the importance of screen locks that protect devices.
- ✓ **Know** how to create passwords that are hard to guess, yet easy to remember.
- ✓ **Choose** the right security for their login settings, including two-factor verification.

Let's talk

Better safe than sorry

Digital technology makes it easy for us to communicate with friends, classmates, teachers, and relatives. We can connect with them in so many ways: via email, text, and instant messages; in words, pics, and videos; using phones, tablets, and laptops. (How do you connect with your friends?)

But the same tools that make it easy for us to share information also make it easier for hackers and scammers to steal that information and use it to damage our devices, our relationships, and our reputations.

Protecting ourselves, our info, and our devices means doing simple, smart things like using screen locks on phones, being careful about putting personal info on unlocked devices that can be lost or stolen, and, above all, building strong passwords.

- Who can guess what the two most commonly used passwords are? (Answer: "1 2 3 4 5 6" and "password.")
- Let's brainstorm some other bad passwords and what specifically makes them bad. (Examples: your full name, your phone number, the word "chocolate.")

Who thinks these passwords are good? **;)**

Continued on the next page →

Activity

Materials needed:

- Internet-connected devices for students or groups of students
- A whiteboard or projection screen
- Handout "Guidelines for creating strong passwords"

Here's an idea for creating an extra-secure password:

- Think of a fun phrase that you can remember. It could be your favorite song lyric, book title, movie catchphrase, etc.
- Choose the first letter or first couple letters from each word in the phrase.
- Change some letters to symbols or numbers.
- Make some letters uppercase and some lowercase.
- Let's practice our new skills by playing the password game.

1. Create passwords

We'll split into teams of two. Each team will have 60 seconds to create a password. (Challenge option: Students share clues with the class first to see how much contextual information the class needs to be able to make an accurate guess.)

2. Compare passwords

Two teams at a time will write their password on the board.

3. Vote!

For each pair of passwords, we'll all vote and discuss whose is stronger.

Takeaway

It's important and fun to create strong passwords.

Guidelines for creating strong passwords

Here are some tips for creating passwords to keep your information safe.

Strong passwords are based on a descriptive phrase or sentence that's easy for you to remember and difficult for someone else to guess – like the first letters in words that make up a favorite title or song, the first letters of words in a sentence about something you did – and include a combination of letters, numbers, and symbols. For example, "I went to Western Elementary School for grade 3" could be used to build a password like: Iw2We$t4g3.

Moderate passwords are passwords that are strong and not easy for malicious software to guess but could be guessed by someone who knows you (for example, IwenttoWestern).

Weak passwords commonly use personal information like a pet's name, are easy to crack, and can be guessed by someone who knows you (for example, "IloveBuddy" or "Ilikechocolate").

DOs

- Use a different password for each of your important accounts.
- Use at least eight characters. The longer the better (as long as you can remember it!).
- Use combinations of letters (uppercase and lowercase), numbers, and symbols.
- Make your passwords memorable so you don't need to write them down, which would be risky.
- Immediately change your password if you know or believe it may be known by someone other than a trusted adult.
- Always use strong screen locks on your devices. Set your devices to automatically lock in case they end up in the wrong hands.
- Consider using a password manager, such as one built into your browser, to remember your passwords. This way you can use a unique password for each of your accounts and not have to remember them all.

DON'Ts

- Don't use personal information (name, address, email, phone number, Social Security number, mother's maiden name, birth dates, etc.), or common words in your password.
- Don't use a password that's easy to guess, like your nickname, just the name of your school, favorite baseball team, a string of numbers (like 123456), etc. And definitely don't use the word "password"!
- Don't share your password with anyone other than your parents or guardian.
- Never write passwords down where someone can find them.

Secure Your Secrets: Activity 2

Keep it to yourself

Teacher uses a school device to demonstrate where to look, and what to look for, when you're customizing your privacy settings.

Goals for students

- ✓ **Customize** privacy settings for the online services they use.
- ✓ **Make decisions** about information sharing on the sites and services they use.
- ✓ **Understand** what two-factor and two-step verifications mean and when to use them.

Let's talk

Privacy equals security

Online privacy and online security go hand in hand. Most apps and software offer ways to control what information we're sharing and how.

When you're using an app or website, look for an option like "My Account" or "Settings." That's where you'll find the privacy and security settings that let you decide:

- What information is visible in your profile
- Who can view your posts, photos, videos, or other content that you share

Learning to use these settings to protect your privacy, and remembering to keep them updated, will help you manage your privacy, security, and safety. It's important to know that your parents or guardian should always be making these decisions with you.

Activity

Materials needed:

- One school device connected to a projector able to display an example account deemed appropriate for class demonstration (e.g., a temporary email or website account)

Review options

I have my school device hooked up to the projection screen. Let's navigate to the settings page of this app, where we can see what our options are. Talk me through (encourage your students to help you)...

- Changing your password
- Going through your sharing, location, and other settings and figuring out which ones are best for you
- Getting alerts if someone tries to log in to your account from an unknown device
- Making your online profile – including photos and videos – visible only to the family and friends you choose
- Enabling two-factor or two-step verification
- Setting up recovery information in case you get locked out of your account

Which privacy and security settings are right for you is something to discuss with your parent or guardian. But remember, the most important security setting is in your brain – you make the key decisions about how much of your personal info to share, when, and with whom.

Continued on the next page →

Takeaway

Choosing a strong, unique password for each of your important accounts is a great first step. Now you need to remember your passwords and keep them private, too.

Secure Your Secrets: Activity 3

Interland: Tower of Treasure

Mayday! The Tower of Treasure is unlocked, leaving the Internaut's valuables like contact info and private messages at high risk. Outrun the hacker and build a fortress with strong passwords to secure your secrets once and for all.

Open a web browser on your desktop or mobile device (e.g., tablet), and visit g.co/TowerOfTreasure.

Discussion topics

Have your students play Tower of Treasure and use the questions below to prompt further discussion about the lessons learned in the game. Most students get the most out of the experience by playing solo, but you can also have students pair up. This may be especially valuable for younger students.

- What are the elements of a super strong password?
- When is it important to create strong passwords in real life? What tips have you learned on how to do so?
- What's a hacker? Describe this character's behaviors and how they affect the game.
- Did playing Tower of Treasure change the way you plan to protect your information in the future?
- Name one thing you'll do differently after learning these lessons and playing the game.
- Craft three practice passwords that pass the "super strong" test.
- What are some examples of sensitive information that should be protected?